UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,907	08/25/2003	Amir Peles	RADW 20.485(101092-00065)	2326

26304 7590 03/26/2007
KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER	
BESROUR, SAOUSSEN	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/647,907	PELES, AMIR	
	Examiner	Art Unit	
	Saoussen Besrour	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 August 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed 8/25/2003.

2. Claims 1-32 were received for consideration.

3. No preliminary amendments for the claims were filed. Currently claims 1-32 are under consideration.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1-6, 8, 9, 10, 12, 13-16, 18-21, 22, 23, 25, 27, 29-31 and 32** are rejected under 35 U.S.C. 102(e) as being anticipated by Hall et al. (US 2003/0018891).

As per **claim 1**, Hall et al. discloses: a. receiving forwarded data packets corresponding to said TCP communication sessions (0019); b. ordering said received data packets and reconstructing session content for each of said one or more sessions (0019); and c. forwarding said reconstructed session content to an external entity (0019).

As per **claim 8**, hall et al. discloses: a. a receiver receiving data packets corresponding to said forwarded encrypted data from said network equipment, ordering

said received data packets for a TCP session, and reconstructing the session content (0019); b. a symmetric session key generator receiving said session content for said TCP session from said receiver, identifying SSL handshake information from said session content, and identifying an encryption scheme and a symmetric session key using said SSL handshake information (0020); c. a decrypter decrypting said session content, said decryption based upon said identified encryption scheme and said identified symmetric key (0020); and d. a forwarder forwarding said decrypted session content to said external entity (0020).

As per **claim 13**, Hall et al. discloses: a. receiving data packets corresponding to said encrypted data, said encrypted data forwarded to said SSL probe from network equipment, said network equipment replicating encrypted data in secure communication sessions between a client and a server, and said forwarded data corresponding to said secure communication sessions (0019); b. ordering said received data packets of a TCP session and reconstructing the session content (0019); c. identifying SSL handshake information from said session content (0020); d. identifying an encryption scheme and a symmetric session key using said identified SSL handshake information (0020); e. decrypting said session content, said decryption based upon said identified encryption scheme and said identified symmetric key (0020); and f. forwarding said decrypted session content to an external entity (0020).

As per **claim 18**, Hall et al. discloses: a. computer readable program code aiding in receiving data packets corresponding to said encrypted data, said encrypted data forwarded to a Secure Sockets Layer (SSL) probe from network equipment, said

network equipment replicating encrypted data in secure communication sessions between a client and a server, and said forwarded data corresponding to said secure communication sessions (0019-0020); b. computer readable program code ordering said received data packets of a TCP session and reconstructing the session content (0020); c. computer readable program code identifying SSL handshake information from said session content (0020); d. computer readable program code identifying an encryption scheme and a symmetric session key using said identified SSL handshake information (0020); e. computer readable program code decrypting said session content, said decryption based upon said identified encryption scheme and said identified symmetric key (0020); and f. computer readable program code aiding in forwarding said decrypted session content to an external entity (0020).

As per **claim 22**, Hall et al. discloses: receiving data packets forwarded to said SSL probe from a network equipment, said network equipment replicating data in a communication session between a client and a server (0019); in said received data packets, selecting and isolating data packets corresponding to encrypted communication sessions (0019- 0020); ordering data packets in said isolated data packets of a TCP session and reconstructing session content (0020); identifying SSL handshake information from said session content; identifying an encryption scheme and a symmetric session key using said identified SSL handshake information (0020); decrypting said session content, said decryption based upon said identified encryption scheme and said identified symmetric key (0020); filtering said decrypted session

content to isolate information pertinent to said external entity (0031-0032); and forwarding said filtered information pertinent to said external entity (0031-0032).

As per **claim 25**, Hall et al. discloses: a receiver receiving data packets corresponding to said forwarded encrypted data from said network equipment, ordering said received data packets of a TCP session and reconstructing session content (0019); a symmetric session key generator receiving said session content from said receiver, identifying SSL handshake information from said session content, and identifying an encryption scheme and a symmetric session key using said SSL handshake information (0020); a decrypter decrypting said session content, said decryption based upon said identified encryption scheme and said identified symmetric key (0020); a filter isolating information pertinent to said external entity via filtering said decrypted session content (0031-0032); and a forwarder forwarding said isolated information pertinent to said external entity (0031-0032).

As per **claim 27**, Hall et al. discloses: a receiver receiving encrypted data packets corresponding to said secure communication session, copying data packets corresponding to said secure session, and for each secure session: ordering said copied data packets, and reconstructing the session content (0019); a session key generator receiving said reconstructed session content from said receiver, identifying SSL handshake information from said session content, and identifying an encryption scheme and a session key using said SSL handshake information (0019-0020); a decrypter decrypting said session content, said decryption based upon said identified encryption scheme and said identified session key (0020); and a forwarder forwarding

said received encrypted data packets to its intended destination and forwarding said decrypted session content to an external entity (0031-0032).

As per **claim 32**, Hall et al. discloses: receiving forwarded data packets corresponding to said TCP communication sessions (0019); and ordering said received data packets and reconstructing session content for each TCP session, and if at least one of said communication sessions is encrypted, then: identifying an encryption scheme and a session key using said reconstructed session content (0020); decrypting said session content, said decryption based upon said identified encryption scheme and said identified session key (0020); and forwarding said decrypted session content to an external entity; else forwarding said reconstructed session content of to an external entity (0020, 0031-0032).

As per **claim 2**, rejected as applied to claim 1. Furthermore, hall et al. discloses: d. identifying, prior to said forwarding step, an encryption scheme and a session key from said reconstructed content (0020); and e. decrypting said session content based upon said identified encryption scheme and said session key, wherein said forwarded session content in (c) is said decrypted session content (0020).

As per **claim 3**, rejected as applied to claim 2. Furthermore, Hall et al. discloses: wherein said at least one encrypted communication session is encrypted via the secure socket layer (SSL) protocol (0020).

As per **claims 4, 9, 14, 19 and 29**, rejected as applied to claims 1, 8, 13, 18, and 27. Furthermore, hall et al. discloses: a filter filtering said generated unencrypted session content to isolate information pertinent to said external entity, and said

forwarder forwarding said isolated information pertinent to said external entity (0031-0032).

As per **claim 5**, rejected as applied to claim 4. Furthermore, Hall et al. discloses: said isolated content represents unencrypted communications from said client (0032).

As per **claim 6**, rejected as applied to claim 4. Furthermore, Hall et al. discloses: said isolated content represents unencrypted communications from said server (0032).

As per **claims 10, 15, 20 and 30**, rejected as applied to claim 8, 13, 18 and 27. Furthermore, Hall et al. discloses: a filter filtering said generated unencrypted session content to isolate unencrypted communications from said client, and said forwarder forwarding said isolated unencrypted communications from said client (0032).

As per **claims 12, 16, 21, and 31**, rejected as applied to claim 8, 13, 18 and 27. Furthermore, Hall et al. discloses: a filter filtering said generated unencrypted session content to isolate unencrypted communications from said server, and said forwarder forwarding said isolated unencrypted communications from said server (0032).

As per **claim 23**, rejected as applied to claim 22. Furthermore, Hall et al. discloses: wherein said step of selecting data packets corresponding to encrypted communication sessions is based upon any of the following selection criteria: IP address of the server, TCP port number of the server, client network range, or an identifier in a data packet (0038).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 7, 11, 17, 24, 26 and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hall et al. (US 2003/0018891) in view of Desrochers et al. (US 2004/0168050).

As per **claims 7, 11, 17, 24, 26 and 28**, rejected as applied to claims 1, 8, 13, 22, 25 and 27. Halls et al. does not explicitly teach wherein said external entity is a network data analysis application. However, Desrochers et al. discloses: wherein said external entity is a network data analysis application (0010-0016, 0026 lines 10-14 and 0027). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Desrochers in conjunction with the teachings of Hall et al. for the benefit of analyzing the decrypted data packets (0016). The modification would have been obvious since Desrochers states in 0027 that the traffic analysis device used can be used for any packet data network having nodes that encrypt and decrypt packet data.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Saoussen Besrour whose telephone number is 571-272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SB
March 19, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100